УДК 519.17

О построении имитационной модели нелинейного обратимого автомата над конечным кольцом

В.В. Скобелев[1]

Abstract – **It is solved the problem of the design of some asymptotically exact imitation model for non-linear one dimensional with the lag 2 automaton over any associative-commutative ring with the unit.**

Key words – **Finite rings, automata, imitation model.**

I. Введение

Интерес к исследованию автоматов над конечным ассоциативно-коммутативным кольцом с единицей обусловлен следующими причинами.

Во-первых, это переход криптографии от чисто комбинаторных моделей к моделям, построенным на основе конечных алгебраических систем [1,2]. При этом практически во всех кандидатах на современные поточные шифры фрагментарно применяются вычисления в кольцах вычетов.

Во-вторых, это проблема обеспечения корректной обратимости процессов при нелинейных преобразованиях в поле рациональных чисел, возникающая при применении хаотических динамических систем [3] к решению задач преобразования информации. Именно для нивелирования этой проблемы естественно перейти к вычислениям в конечной алгебраической системе.

Обратимый автомат над конечным ассоциативно-коммутативным кольцом с единицей является математической моделью симметричного поточного шифра. Поэтому для такого автомата сложность решения задач параметрической идентификации и распознавания вектора начального состояния является теоретической аргументацией вычислительной стойкости шифра. В [4] показано, что решение этих задач сводится к поиску решения систем уравнений над кольцом. Такие системы уравнений могут иметь не единственное решение.

В то же время, одной из разновидностей атаки на шифр является попытка построения криптоаналитиком, на основе полученной им информации, алгоритма, который достаточно хорошо осуществляет как шифрование, так и расшифровку. Такой алгоритм естественно назвать имитационной моделью. Для блочных шифров имитационные модели могут быть получены в результате дифференциального или интегрального анализа.

В настоящей работе рассматривается задача построения имитационной модели для нелинейного одномерного с лагом 2 автомата над ассоциативно-коммутативным кольцом $(K,+,\cdot)$ с единицей.

II. Основные понятия

Пусть M – автомат, заданный над кольцом $(K,+,\cdot)$ системой уравнений, зависящей от набора параметров $\vec{a}=(a_1,\dots,a_l)$, у которого K^n – множество состояний, а K^m – как входной, так и выходной алфавит.

Зафиксируем отображение

$$g_{\vec{a}} : (K^m)^+ \to (K^m)^+ . \qquad (1)$$

Рассмотрим отображение

$$f_{(M,\vec{q}_0)} : (K^m)^+ \to (K^m)^+ ,$$

реализуемое инициальным автоматом $(M,\vec{q}_0)$ $(\vec{q}_0 \in K^n)$.

Пусть для входного слова $\vec{x}_1 \dots \vec{x}_k \in K^{mk}$

$$g_{\vec{a}}(\vec{x}_1 \dots \vec{x}_k) = \vec{v}_1 \dots \vec{v}_k$$

и

$$f_{(M,\vec{q}_0)}(\vec{x}_1 \dots \vec{x}_k) = \vec{u}_1 \dots \vec{u}_k .$$

Обозначим через $d_{\vec{q}_0,\vec{x}_1\dots\vec{x}_k}(\vec{v}_1 \dots \vec{v}_k)$ длину слова, полученного в результате вычеркивания из слова $\vec{v}_1 \dots \vec{v}_k$ всех таких символов $\vec{v}_i$, что $\vec{v}_i \neq \vec{u}_i$ и положим

$$\alpha_{\vec{q}_0,k} = \frac{\sum_{\vec{x}_1\dots\vec{x}_k \in K^{mk}} d_{\vec{q}_0,\vec{x}_1\dots\vec{x}_k}(\vec{v}_1 \dots v_k)}{|K|^{mk}} ,$$

$$\beta_{\vec{q}_0} = \lim_{k\to\infty} \frac{1}{k} \sum_{i=1}^{k} \alpha_{\vec{q}_0,k}$$

и

$$\gamma = \min_{\vec{q}_0 \in K^n} \beta_{\vec{q}_0} .$$

Отображение (1) назовем имитационной моделью автомата M, осуществляющей моделирование автомата M с точностью, равной γ.

Если $\gamma = 1$, то назовем имитационную модель (1) асимптотически точной.

III. Асимптотически точная модель для одного класса нелинейных автоматов

Рассмотрим над ассоциативно-коммутативным кольцом $(K,+,\cdot)$ с единицей класс A нелинейных одномерных обратимых автоматов Мура M с лагом 2, определяемых системой уравнений

$$\begin{cases} q_{t+2} = a + b\cdot q_{t+1}^2 + c\cdot q_t + d\cdot x_{t+1} \\ y_{t+1} = e\cdot q_{t+2} \end{cases} , \qquad (2)$$

[1] Институт прикладной математики и механики НАН Украины, ул. Розы Люксембург, 74, Донецк, 83114, Украина
E-mail: vv_skobelev@iamm.ac.donetsk.ua

где x_{t+1} и y_{t+1} – соответственно, входной и выходной символ в момент $t+1$, $\vec{q}_t = (q_{t+1}, q_t)$ – состояние в момент t, а a, b, c, d, e – параметры, причем $a, b, c \in K \setminus \{0\}$, а $d, e \in K$ – обратимые элементы кольца.

Отметим, что уравнение

$$q_{t+2} = a + b \cdot q_{t+1}^2 + c \cdot q_t$$

Представляет собой аналог над кольцом $(K,+,\cdot)$ ряда модельных хаотических отображений, в том числе, отображения Эно [3].

Для автомата (2) обратный автомат имеет вид

$$\begin{cases} q_{t+2} = e^{-1} \cdot x_{t+1} \\ y_{t+1} = d^{-1} \cdot (e^{-1} \cdot x_{t+1} - a - b \cdot q_{t+1}^2 - c \cdot q_t) \end{cases}. \quad (3)$$

При использовании пары автоматов (2) и (3) в качестве модели симметричного поточного шифра параметры являются секретным ключом большой длительности, а начальное состояние – секретным сеансовым ключом.

Отметим, что в процессе шифрование-расшифровка автоматы (2) и (3) движутся в пространстве состояний по одной и той же траектории в одном и том же направлении.

Из (2) вытекает, что

$$y_{t+1} = e \cdot (a + b \cdot q_{t+1}^2 + c \cdot q_t + d \cdot x_{t+1}). \quad (4)$$

Подставив $t = 0,1,\ldots,k$ $(k > 2)$ в (4), с учетом второго уравнения системы (2), получим

$$\begin{cases} y_1 = e \cdot a + b \cdot e \cdot q_1^2 + c \cdot e \cdot q_0 + e \cdot d \cdot x_1 \\ y_2 = e \cdot a + b \cdot e^{-1} \cdot y_1^2 + c \cdot e \cdot q_1 + e \cdot d \cdot x_2 \\ y_i = e \cdot a + b \cdot e^{-1} \cdot y_{i-1}^2 + c \cdot y_{i-2} + e \cdot d \cdot x_i \quad (i = 3,\ldots,k) \end{cases}. \quad (5)$$

Анализ системы уравнений (5) дает возможность доказать следующую теорему.

Теорема. Никакой простой или кратный эксперимент с автоматом $M \in A$ не дает возможность вычислить точное решение задачи его параметрической идентификации. Однако может существовать простой, либо кратный эксперимент с автоматом $M \in A$, который даст возможность построить асимптотически точную имитационную модель автомата M, причем только параметр $c \in K$ будет вычислен точно.

В том случае, когда указанная в теореме асимптотически точная имитационная модель автомата $M \in A$ существует, она имеет следующий вид: в качестве значений y_1 и y_2 выбираются фиксированные элементы кольца, а для всех значений $i > 2$

$$y_i = e \cdot a + b \cdot e^{-1} \cdot y_{i-1}^2 + c \cdot y_{i-2} + e \cdot d \cdot x_i. \quad (6)$$

Из (6) вытекает, что для всех значений $i > 2$

$$x_i = (e \cdot d)^{-1} \cdot (e \cdot a + b \cdot e^{-1} \cdot y_{i-1}^2 + c \cdot y_{i-2} - y_i). \quad (7)$$

Значение равенств (6) и (7) состоит в следующем. Если криптоаналитик может вычислить из системы уравнений (5) значения величин

$$e \cdot a, b \cdot e^{-1}, c, e \cdot d,$$

то он будет корректно осуществлять как шифрование, так и расшифровку всех суффиксов, полученных при отбрасывании префиксов длины 2.

Таким образом, автомат $M \in A$, как математическая модель, может использоваться в поточном шифре S только для шифрования предварительно зашифрованной информации, причем только, если секретный сеансовый ключ содержится в первых двух символах шифруемой последовательности.

При этом использование автомата $M \in A$ не повышает вычислительную стойкость шифра S.

III. Выводы

Полученные результаты показывают, что в процессе построения асимптотически точной имитационной модели автомата $M \in A$ экспериментатор вынуждении осуществлять поиск по множеству, содержащему не менее чем $|K|^4$ входных слов.

Отсюда вытекает, что сложность построения асимптотически точной имитационной модели автомата $M \in A$ высока (достаточно рассмотреть кольцо вычетов по модулю p^k, где p – простое число, для записи которого требуется, по крайней мере, 100 бит).

Тем не менее, построенная асимптотически точная имитационная модель имеет достаточно простой вид. Это обусловлено тем, что функция выходов автомата $M \in A$ является линейной функцией от одной из компонент состояния автомата.

Выделение классов обратимых автоматов над ассоциативно-коммутативным кольцом с единицей, для которых любая асимптотически точная имитационная модель существенно сложнее, чем система уравнений, определяющая автомат, является возможным направлением дальнейших исследований. Другое направление связано с исследованием классов обратимых автоматов, для которых обращение асимптотически точной имитационной модели либо не является асимптотически точной имитационной моделью обратного автомата, либо расшифровывает фрагменты шифртекста, удаленные друг от друга.

Литература

[1] А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин и др. Основы криптографии. М.: Гелиос АРВ, 2002. 480 с.

[2] Ю.С. Харин, В.И. Берник, Г.В. Матвеев и др. Математические и компьютерные основы криптологии. Минск: Новое знание, 2003. 382 с.

[3] С.П. Кузнецов. Динамический хаос. М.: Физматлит, 2001. 296 с.

[4] В.В. Скобелев, В.Г. Скобелев. Анализ шифрсистем. Донецк: ИПММ НАН Украины, 2009. 479 с.